

DUPLICATE FILE COPY ORIGINAL

Received & Inspected

2/22/2010

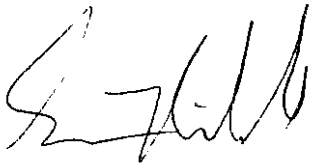
FEB 25 2010

FCC Mail Room

To Whom It May Concern-

Enclosed are the CPNI Certifications for Datalytix, LLC (FCC Filer ID 826468) for 2010.

Note that Datalytix, LLC has no end users, and thus never provides CPNI to customers. Datalytix, LLC only uses call detail for billing purposes, and never provides access to CPNI to anyone for any reason. I have filled out the annual statements reflecting the fact that Datalytix, LLC has no end users. I have attached our CPNI policy, which covers issues that we do not currently face, as we have no end users.



Sean Riddle

Vice President

Datalytix, LLC

No. of Copies rec'd 0+4
Lit. ACODE

Received & Inspected

FEB 25 2010

FCC Mail Room

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2010

Date filed: February 22, 2010

Datalytix, LLC

Form 499 Filer ID: 826468

Name of signatory: Sean Riddle

Title of signatory: Vice President

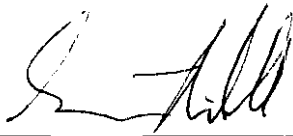
I, Sean Riddle, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions (proceedings instituted or petitions filed by a Company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed: _____



Statement Concerning the Protection of Customer Proprietary Network Information for the Annual Period Ending December 31, 2009

1. Datalytix, LLC, ("Company") is a telecommunications carrier subject to the requirements set forth in Section 64.2009 of the Federal Communications Commission's ("FCC's") rules. Company has established policies and procedures to satisfy compliance with the FCC's rules pertaining to use, disclosure and access to customer proprietary network information ("CPNI") set forth in sections 64.201 et. seq.
2. Company has no end users. Company's only customer is another carrier also subject to the CPNI rules. Many of the following statements assume Company has end users. Company has no plans to sell long distance directly to end-users, but if those plans change, Company will comply with all CPNI rules and file another certification.
3. If anyone calls Company requesting information that is considered CPNI, Company does not release such information.
4. Company does not use, disclose or permit access to CPNI to provide or market service offerings.
5. Information protected by Company includes information that relates to the quantity, technical configuration, type, destination, location and amount of use of all telecommunications services made available to Company by the customer solely by virtue of the carrier-customer relationship. Also protected is information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer.
6. Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.
7. Company never uses or releases any CPNI to anyone for any reason.
8. Company personnel are trained to never release or use CPNI, and violation of these rules will subject personnel to express disciplinary action.
9. Company has never used, disclosed, or accessed CPNI for any reason other than to provide service and billing. If customer approval to use, disclose, or permit access to customer CPNI is ever desired, Company will obtain such customer approval through written or oral methods (however, we only utilize the oral authorization to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts, and such CPNI authority, if granted, lasts only for the duration of that specific call). Company honors a customer's approval or disapproval until the customer revokes or limits such approval or disapproval.
10. Company never uses any CPNI for outbound marketing.

11. Prior to any solicitation for customer approval, Company will provide notification to customers of their right to restrict use of, or disclosure of, and access to the customer's CPNI. Records of these notifications will be maintained for a period of at least one year.
12. Company's notifications will provide information sufficient to enable customers to make informed decisions as to whether to permit the use or disclosure of, or access to, their CPNI. Company's notifications will: (1) contain a statement that the customer has a right, and Company has a duty under federal law, to protect the confidentiality of CPNI; (2) specify the types of information that constitute CPNI and the specific entities that will receive the CPNI; (3) describe the purposes for which the CPNI may be used; and (4) inform the customer of the right to disapprove those uses and deny or withdraw access to or use of CPNI at any time.
13. Company's notifications will inform the customer that any approval or denial of approval for the use of CPNI outside of the service to which the customer already subscribes is valid until the customer affirmatively revokes or limits such approval or denial.
14. Company will advise its customers of the precise steps the customer must take in order to grant or deny access to CPNI, and that denial of approval will not affect the provision of any services to which the customer subscribes.
15. Company has never had sales and marketing campaigns that use customer's CPNI. CPNI has never been disclosed or provided to third parties and no third parties have ever been allowed access to CPNI.
16. Company never discloses CPNI to any joint venture partner or independent contractor.
17. If a breach of CPNI occurs, Company will provide electronic notification of the breach to the U.S. Secret Service and the FBI within seven (7) days. Company will also notify customer after seven (7) more days unless there is a risk of immediate and irreparable harm to the customer in which case Company will notify the customer immediately. Company will keep records of discovered breaches for at least two (2) years.
18. Company takes care that its computers and network are reasonably protected from intrusion. The computers are located in a private facility that is locked and protected by a security system when Company employees are not present. The computers are protected by hardware and software firewalls, as well as anti-virus and anti-spyware software. The computers that process call records do not run email clients or web browsers, so the chances of those computers becoming infected in the first place is very low.

CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC ("Carrier")

(i.e., a local exchange Carrier may not use local service CPNI to track all customers that call local service competitors.) Carrier may not release CPNI to a third party without the written consent of the customer. All marketing plans developed by Carrier's employees or on behalf of Carrier must address the use of CPNI and be approved by the officer or employee responsible for CPNI compliance ("CPNI Compliance Officer").

Carrier's policy dictates that failure to abide by these policies and procedures could result in disciplinary action or termination.

Use of CPNI

"Authorized" CPNI is CPNI that Carrier *has provided customer notification and obtained opt-in authorization prior to its use for marketing purposes.* Under the FCC's rules, for Carrier to market communications-related services outside of the customer's subscribed service (outside the total service approach), Carrier must provide notification to the customer and obtain opt-in authorization from the customer for the use of such CPNI to market other services.

Carrier may obtain authorization for the use of CPNI through written, oral or electronic methods. A Carrier relying on oral approval bears the burden of demonstrating that such approval has been given. Customer approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval. Carrier must maintain records of approval or disapproval by oral, written or electronic means, for at least one year.

Carrier may, subject to customer through opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer.

Carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services.

A telecommunications Carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section §64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications Carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

Joint Venture/Contractors Safeguards

Carrier must obtain opt-in approval prior to sharing customer's CPNI with Carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer. To the extent that Carrier voluntarily obtained opt-in approval from their customers for the disclosure of customer's CPNI to joint venture partners or independent contractor for the purposes of marketing communications-related services to a customer prior to the adoption of the new CPNI rules, Carrier can continue to use those approvals. If Carrier discloses or provides access to CPNI to its joint venture partners or independent contractors they must enter into confidentiality agreements that state such joint venture or contractor will use the CPNI only for the purpose of marketing or providing the communications-related service for which that CPNI has been provided. The agreement must also state that the independent contractor or joint venture partner will not use, allow access to, or disclose the CPNI to any other party, unless required to make such disclosure under force of law. Such joint venture partner or contractor must implement appropriate safeguards to ensure the ongoing confidentiality of CPNI.

Notice Required for Use of CPNI

Prior to any solicitation for customer approval, Carrier must provide notification to the customer of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. Carrier must maintain written record of the notification for at least one year. Individual notice to customers must be provided when soliciting approval to use, disclose or permit access to a customer's CPNI.

CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC ("Carrier")

The notice must include sufficient information to enable the customer to make an informed decision as to whether to permit a Carrier to use, disclose, or permit access to, its CPNI. The notification must state that the customer has a right, and the Carrier has a duty under federal law to protect the confidentiality of CPNI. The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time. The notification must advise the customer of the precise steps the customer must take to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes.

Carriers may provide a brief statement in clear and neutral language, describing the consequences directly resulting from the lack of access. The notification must be clear and not misleading. The notification may state that the customer's approval of the use of CPNI may enhance the Carrier's ability to offer products and services tailored to the customer's needs. The notification may also state that Carrier may be compelled to disclose CPNI to any person upon affirmative written request by the customer. Carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI. The notification must state that any approval or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that Carrier is valid until the customer affirmatively revokes or limits such approval or denial. Carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

Notice Requirements Specific to Opt-in

Carrier may provide notification to obtain opt-in approval through oral, written or electronic methods. The notice must comply with the notice requirements listed above.

Notice Requirement Specific to One-Time Use of CPNI

Carrier may use oral notice to obtain limited, one-time use of CPNI for inbound and out-bound customer telephone contacts for the duration of the call, regardless of whether the Carrier uses opt-in approval based on the nature of the contact. The contents of such notification must comply except that Carrier may omit any of the following notice provision if not relevant to the limited use for which the Carrier seeks CPNI. Carrier need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election. Carrier need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by or disclosure to, an affiliate or third party. Carrier need not disclose the means by which a customer may deny or withdraw future access to CPNI so long as Carrier explains to customers that the scope of the approval it seeks is limited to one time use. Carrier may omit disclosure of the precise steps a customer must take to grant or deny access to CPNI as long as Carrier clearly communicates that the customer can deny access to his CPNI for the call.

Company CPNI Safeguards

Carrier must maintain a system whereby the status of a customer's CPNI approval status can clearly be established prior to the use of CPNI. All personnel of Carrier with access to CPNI must be educated and trained as to when CPNI may be used and when it may not be used. All personnel with access to CPNI must fully understand the FCC's rules regarding CPNI. Carrier has an express disciplinary process in place for employees that do not follow Carrier's CPNI policies and procedures and such process could result in employment termination. Carrier maintains records of all its marketing campaigns and its affiliate's marketing campaigns that use their customers' CPNI. The record includes a description of the marketing campaign, the specific CPNI used, and the products and services that were part of the campaign. Carrier maintains records of instances where CPNI was disclosed or provided to third parties, or where third parties were given access to CPNI. All records are maintained for at least one year. Carrier has implemented a supervisory review process regarding its compliance with the FCC's rules for outbound marketing situations and maintains records of Carrier's compliance for a minimum of one year.

Annual CPNI Certification.

Carrier has appointed an officer, as an agent of the Carrier, to annually certify that he or she has personal knowledge that Carrier has established operating procedures that are adequate to ensure compliance with the

CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC ("Carrier")

FCC's CPNI rules. Along with this certification, Carrier must provide a statement explaining how Carrier's operating procedures ensure that it is in compliance with the FCC's rules regarding use of CPNI. In addition, Carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. By "any action", Carrier must report on proceedings instituted or petitions filed by a Carrier at either state commissions, the court system, or at the FCC against data brokers. For the summary of customer complaints, Carrier must report on the number of customer complaints it received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaint (e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by unauthorized individuals). Additionally, Carriers must report on information that they have with respect to the processes pretexters are using to attempt to access CPNI and steps taken to protect CPNI. Carrier must file this certification and accompanying statement annually with the Enforcement Bureau of the FCC on or before March 1 for data pertaining to the previous calendar year.

Safeguards on the Disclosure of CPNI

Carrier must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Carrier must properly authenticate a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-office visit. Carrier may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the Carrier asking for readily available biographical information or account information. If the customer does not remember their password, Carrier always asks the backup question. If a customer does not provide a password or the correct answer to the backup question, Carrier may only disclose call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the customer is able to provide call detail information during a customer-initiated call without Carrier's assistance, then Carrier is permitted to discuss the call detail information provided by the customer. *Call detail or call records* includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location or duration of any call. While a customer's remaining minutes is NOT call detail; it is still CPNI. *Readily available biographical information* is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number, the customer's mother's maiden name, a home address or a date of birth. *Account information* is information specifically connected to the customer's service relationship and includes such things as an account number or any component, the telephone number associated with the account or the amount of the last bill. An address of record, whether postal or electronic, means an address that the Carrier has associated with the customer's account for at least 30 days. *Address of record* is, whether postal or electronic, an address that the Carrier has associated with the customer's account for at least 30 days. The *telephone number of record* means the telephone number associated with the underlying service, rather than some other number supplied as a customer's contact information. CARRIER may disclose non-call detail CPNI to a customer after Carrier authenticates the customer (i.e., no password is required for non-call detail); however, Carrier is still subject to Section 222's duty to protect CPNI and thus must authenticate a customer prior to disclosing non-call detail.

Establishment of Password Protection.

For a new customer (a customer that establishes service on or after December 8, 2007, the effective date of the new CPNI rules), Carrier must request that the customer establish a password at the time of service initiation. For existing customers to establish a password, Carrier must first authenticate the customer without the use of readily available biographical information or account information. Carriers must authenticate a customer using non-public information. For example, a Carrier could call the customer at the telephone number of record.

Carrier may use a Personal Identification Number (PIN) method to authenticate a customer. A randomly generated PIN may be supplied to customer, not based on readily available biographical information or account information, which the customer would then provide to the Carrier prior to establishing a password. Carrier could supply a PIN to the customer by a Carrier-originated voicemail or text message to the telephone number of record, or by sending it an address of record to ensure that it is delivered to the intended party.

CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY DataLytx, LLC ("Carrier")

Use of Password Protection.

For accounts that are password protected, Carrier cannot obtain the password by asking for readily available biographical information or account information to prompt the customer for his password. Carrier uses a backup question/response if the password is forgotten. A customer may also access call detail information by establishing an online account or by visiting a Carrier's location. If a password is forgotten or lost, Carrier may create back-up customer authentication methods that are not based on readily available biographical information or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

Alternative Access to Call Detail Information.

If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking Carrier to send the call detail information to an address of record or by the Carrier calling the telephone number of record. In addition, if a customer is able to provide to the Carrier, during a customer initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and if applicable, the amount charged for the call) then Carrier is permitted to proceed with its routine customer care procedures. Under these circumstances, Carrier may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.

Online Account Access.

Carrier must password-protect online access to all CPNI, call detail and non-call detail. Online account access allows a customer to view and change personal information easily, including online passwords, addresses of record and billing information without Carrier assistance. The online account access rules include the disclosure of all CPNI to protect privacy.

Carrier may not rely on readily available biographical information or account information to authenticate a customer's identity before a customer accesses CPNI online. Carrier must authenticate both new and existing customers seeking access to CPNI online. Carrier may request a customer establish an online password at the time of service initiation. Alternatively, for all customers, Carrier could use a PIN method to authenticate customers. If a customer cannot provide a password or the proper response for the backup authentication method to access an online-account, Carrier must re-authenticate the customer based on the authentication methods described above.

Carrier Location Account Access.

Carrier may provide customers with access to CPNI at Carrier's location if the customer presents a valid photo ID and the valid photo ID matches the name on the account. Valid photo ID means a government issued personal identification with photograph such as a current driver's license, passport or comparable ID.

Notice to Customer of Account Changes.

Carrier must notify a customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a Carrier originated voicemail or text message to the telephone number of record, or by mail to the address of record, so as to reasonably ensure that the customer receives this notification, and must not reveal the changed information or be sent to the new account information.

Business Customer Exception.

If Carrier's contract with a business customer is serviced by a dedicated account representative as the primary contact, and specifically addresses the Carrier's protection of CPNI, the Carrier authentication rules do not apply to these business customers because businesses are typically able to negotiate appropriate protection of CPNI in their service agreements. However, all CPNI rules apply. ***If the business customer must go***

**CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC
("Carrier")**

through a call center to reach a customer service representative than this exemption does not apply to that customer.

Notice of Unauthorized Disclosure of CPNI.

In the event of a CPNI breach (a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI), Carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph. Specifically, Carrier must notify law enforcement of a breach of its customers' CPNI no later than seven (7) business days after making a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the FBI. The Carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification. Notwithstanding any state law to the contrary, Carrier may notify the customer and/or disclose the breach publicly after seven (7) business days following notification to the USSS and FBI, if the USSS and the FBI have not requested that the Carrier continue to postpone disclosure.

If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, that agency may direct Carrier not to disclose the breach for an initial 30-day period. This 30-day period may be extended by the law enforcement agency as reasonably necessary. If such direction is given, the agency shall notify the Carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The law enforcement agency must provide in writing to Carrier its initial direction and any subsequent direction/extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by Carriers. Carrier, however, may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if Carrier believes there is an extraordinarily urgent need to notify a customer or class of customers to avoid immediate and irreparable harm. Additionally, Carrier must maintain a record of any discovered breaches and notifications to the customers, the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two years. This record must include, if available, the date that Carrier discovered the breach, the date Carrier notified the USSS and the FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach. The FCC maintains a link to the reporting facility at www.fcc.gov/eb/cpni.

CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC ("Carrier")

SAMPLE CUSTOMER NOTICE - MUST BE CLEAR AND IN LARGE TYPE

Important Customer Notice

Federal law protects your privacy rights as a customer of Datalytix, LLC ("Carrier"). These rights are in addition to the existing safeguards that Carrier already has in place to ensure your privacy rights. The Federal Communications Commission (FCC) requires Carrier to notify you as a subscriber of your right to restrict the use of, disclosure of, and access to your Customer Proprietary Network Information (CPNI). **You have the right, and Carrier has a duty, under Federal law, to protect the confidentiality of your CPNI.**

CPNI: CPNI is information you might consider private and therefore wish for Carrier to protect it from use for marketing purposes. CPNI is information Carrier possesses solely due to the customer-Carrier relationship that is necessary for Carrier to serve your telecommunications needs. CPNI is defined by the FCC as information that relates to the quantity, technical configuration, type, destination and amount of use of a telecommunications service subscribed to by any customer of a telecommunications Carrier and that is made available to the Carrier by the customer solely by virtue of the Carrier-customer relationship; and information contained in the bills pertaining to telephone exchange or toll service received by a customer of a Carrier. CPNI does not include information that is in the public domain or available from other, non-Carrier sources. For example, census data, subscriber list information and published directory information is public data.

EXAMPLES OF CPNI: Examples of CPNI include Carrier knowledge of the types of services to which you subscribe such as Caller ID, the quantity of your calls or the amount of your long distance bill or a list of phone numbers you have called. In other words, CPNI is information about when, where and how often a customer makes use of telecommunications services.

PERMITTED USE OF CPNI BY COMPANY WITHOUT YOUR PERMISSION

CPNI can be used by Carrier for certain purposes without your permission. Carrier may use CPNI to offer you new or enhanced services that are related to the category of services to which you currently subscribe. Carrier may also use CPNI to respond to your inquiry regarding services you currently use or related services Carrier offers. In addition, Carrier may use CPNI in connection with repair and maintenance services, billing and collection, to protect company property and to prevent fraud.

PROHIBITED USE OF CPNI UNLESS AUTHORIZED BY YOU

Unless you specifically authorize its use, Carrier may not use CPNI to market its services that are unrelated to the services to which you currently subscribe. For example, Carrier may not use CPNI to offer you any type of long distance or wireless service unless you currently subscribe to such long distance or wireless services. Carrier may not share CPNI with any other company, including affiliate companies unless you are also a customer of the affiliate.

ADDITIONAL INFORMATION REGARDING YOUR CPNI RIGHTS You have the right to deny or withdraw access to CPNI at any time or to instruct Carrier to disclose CPNI to unaffiliated third parties upon the submission of a written request. Any approval or denial for the use of CPNI outside of the service to which you subscribe to from Carrier is valid until you affirmatively revoke or limit such approval or denial. A denial of your approval will not affect the provision of any services to which you subscribe.

**CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC
("Carrier")**

SAMPLE CUSTOMER CPNI AUTHORIZATION

CPNI Customer Authorization for Release of CPNI to Affiliates of Company, Joint Venture Partners or Independent Contractors or Third Party Telecommunications Carriers

I, _____, hereby authorize Datalytix, LLC ("Carrier") to release any information in its possession and protected under Federal CPNI rules to:

- (1) its affiliates for use in connection with the marketing of communications-related services or telecommunications services; [or]
- (2) its joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer; [or] _____ (third party).

Carrier has provided me clear notification as to my rights to restrict the use of, disclosure of, and access to my CPNI under Federal law. I fully understand my rights to restrict the use of, disclosure of, and access to my CPNI. I also understand my rights to limit or revoke this authorization at any time upon proper notice to Carrier.

Signed _____

Date _____

**CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC
("Carrier")**

SAMPLE LETTER TO AGENTS CONCERNING NEW CPNI REQUIREMENTS

To: All Agents of Datalytix, LLC, ("Carrier")

Re: Agent Notification of new CPNI Rules and Procedures

New rules have recently been adopted by the FCC concerning the use of customer proprietary network information ("CPNI"). The new rules are intended to better protect and prevent unauthorized access and disclosure of CPNI. CPNI includes information such as quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by a customer, along with billing information pertaining to that telephone service.

In order for you to continue to act of behalf of a customer of Carrier, you will be required to provide us with a customer signed Authorization on customer letterhead. A sample letter to customers and an authorization form are attached to this Notification. You will not be provided any customer information until we receive properly executed Authorizations from the customer.

Should a third party gain unauthorized access to CPNI which has been released to you pursuant to a properly executed Authorization from a customer, you are required to notify Carrier immediately in order for Carrier to fulfill the notification requirements of the new rules.

You are further notified that any prohibited disclosure by Agent of CPNI that subjects Carrier to assessment of any fines or penalties will be deemed a breach of the Confidentiality and Non-Disclosure provisions of your agreement with Carrier and Agent will be held responsible for all such fines or penalties including costs of contract enforcement.

Should you have any questions concerning these new rules and procedures, please contact us at (405) 706-3427.

Sincerely,

**CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC
("Carrier")**

SAMPLE LETTER FROM AGENT TO CUSTOMER

Re: New FCC Mandated CPNI Requirements

Dear Customer:

New FCC rules intended to better protect and prevent unauthorized access and disclosure of CPNI have recently gone into effect. These rules prohibit the disclosure of CPNI to third parties unless the customer has specifically authorized the release of said information. CPNI includes information such as quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by a customer, along with billing information pertaining to that telephone service.

If you wish us to continue to represent you with Datalytix, LLC ("Carrier"), please copy the attached Authorization Form onto your company letterhead, sign and return to me as soon as possible. Until receipt of your signed authorization, we will not have access to your CPNI and will be unable to continue to assist you with new service ordering, trouble tickets, billing disputes or other services requiring our access to your specific information.

Should you have any questions concerning the new rules or the Authorization Form, please contact us at (405) 706-3427.

Sincerely,

**CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY Datalytix, LLC
("Carrier")**

SAMPLE AUTHORIZATION FORM

AUTHORIZATION FOR THIRD-PARTY ACCOUNT REPRESENTATION

I, _____, hereby authorize Datalytix, LLC ("Carrier") to release any information in its possession and protected under Federal CPNI rules to _____ ("Agent").

This letter of Authorization applies to the following:

Check as appropriate:

_____ This service order only.

_____ The full term, including extensions, of the contract with Carrier unless Carrier is notified in writing of the revocation of this Authorization.

Carrier may deal directly with Agent with regards to all matters, including product and service changes or additions, billing dispute resolution, processing of trouble tickets, etc. unless noted below:

This Authorization does not preclude Carrier from dealing directly with me or employees of my company if specifically authorized by me, with regards to any matter in which they may also deal with Agent pursuant to this Authorization.

Customer/Business Name: _____

Address: _____

Printed Name of Authorized
Representative:

Authorized Signature:

Title:

Date:
